		r			
Application & Interface Security		AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes	We use automatic security scan tools for code, dependencies and artifacts.
	Application Security	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes	
	Customer Access Requirements	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes	We make sure that these specific requirements (E.g. GDPR and related) are covered in the customer agreement and privacy policy.
			Does your data management policies and procedures require audits to verify	Yes	Data input is validated prior to ingestion and API outputs are sanitized.
	Data Integrity	AIS-03.1	data input and output integrity routines?		Data input is valuated prof to ingestion and Ai Fourputs are sanitized.
Audit Assurance & Compliance		AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Yes	
	Independent Audits	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Yes	Pentest third party report available by request
		AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure	Yes	Pentest third party report available by request
	Information System Regulatory Mapping	AAC-03.1	program for changes to legal requirements, and ensure compliance with	Yes	Our IT/DPO office monitors for regulatory requirement changes
Business Continuity Management & Operational Resilience	Business Continuity Testing	BCR-02.1		Yes	We review our business continuity plan on an annual basis (or upon significant organizational and environmental change) and make changes to our internal policies &
	Policy	BCR-10.1	effectiveness? Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes	documentation as a result, as part of our ISMS process. Documentation is updated regularly and our engineers rotate in support roles frequently with regular trainings and knowledge sharing sessions to ensure the support
	Retention Policy	BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	Yes	procedures are known and applied consistently The customer agreement outlines the data retention policy and we can enforce this as required.
		BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes	
		BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	Yes	At least twice a year.
Change Control & Configuration	Unauthorized Software		Do you have controls in place to restrict and monitor the installation of	Yes	Provisioning of infrastructure is automated through reviewed code, and previous instances
Management	Installations	CCC-04.1	unauthorized software onto your systems?		are replaced.
Data Security & Information Lifecycle Management	E-commerce Transactions	DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes	All integration flows use encrypted protocols.
		DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes	All integration flows use encrypted protocols.
	Nonproduction Data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	No	Some data from production, as stipulated in the customer agreement, may be used to train our AI models which may be used for testing purposes on other protected environments.
		DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	Yes	Our cloud providers support secure deletion of data.
	Secure Disposal	DSI-07.2	arcmwo and backee-up data? Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes	
Datacenter Security	Asset Management	DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	Yes	We do not maintain a datacenter. Digitally critical assets and their ownership are listed in the asset inventory and business continuity plan.
	Controlled Access Points	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	Not Applicable	We do not host sensitive data on-prem, our cloud providers support physical security perimeters.
	User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users	Not Applicable	
Encryption & Key Management				Not Applicable Yes	Customer-provided files and customs proposal output is encrypted at rest in separate
Encryption & Key Management	Key Generation	EKM-02.1	Do you restrict physical access to information assets and functions by users and support personnel?		
Encryption & Key Management Governance and Risk Management			Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS	Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed.
	Key Generation Encryption	EKM-02.1 EKM-03.1 GRM-	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? Are your information security policies and procedures made available to all	Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed.
	Key Generation Encryption	EKM-02.1 EKM-03.1 GRM-	Do you restrict physical access to information assets and functions by users and support personnet? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you encrypt tenant data at rest (on disk/storage) within your environment? of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers
	Key Generation Encryption Baseline Requirements	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 06.1 GRM-	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by a accumtable business rold/nuclican and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have	Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers
	Key Generation Encryption Baseline Requirements Policy Policy Enforcement	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 06.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you encrypt tenant data at rest (on disk/storage) within your environment? do you infastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you molty you tenants when you make material changes to your information security and/co privacy policies?	Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified.
Governance and Risk Management	Key Generation Encryption Baseline Requirements Policy	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 06.1 GRM- 07.1 GRM-	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by a accountable business roldruiccion and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you notify von tenants when your make material changes to your information security and/or privacy policies? Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified.
	Key Generation Encryption Baseline Requirements Policy Policy Enforcement	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 06.1 GRM- 07.1 GRM- 09.1 GRM-	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per indust/ best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you notify your tenants when you make material changes to your information security and/or privacy policies? Do you perform, at minimum, annual reviews to your privacy and security policies? Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning oraanzaitonality-owned assets?	Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified.
Governance and Risk Management	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 06.1 GRM- 09.1 GRM- 09.2	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/nuclion and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security and/or privacy policies? Do you portiny at minimum, annua reviews to your privacy and security pacifies? Upon termination of contract or business relationship, are employees and business partners adequately informed of ther obligations for returning organizationally-word assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to backgrount verifection?	Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified.
Governance and Risk Management	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews Asset Returns	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 05.1 GRM- 09.1 GRM- 09.2 HRS-01.1 HRS-02.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, nouters, DNS servers, et.)? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business roldruiccion and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you notify your lenants when you make material changes to your information security and/or privacy policies? Upon termination of contract or business relationship, are employees and business rolaritomed of the informations for returning organizationally-owned assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to	Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified.
Governance and Risk Management	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Employment	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 05.1 GRM- 09.1 GRM- 09.2 HRS-01.1 HRS-02.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/unction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security noticies and procedures? Do you portfyrou tenants when your make material changes to your information security and/or privacy policies? Do you perform, at minimum, annual reviews to your privacy and security policies? Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning arganizationally-owned assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies? Are documented policies, procedures, and guidelines in place to govern	Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified.
Governance and Risk Management	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Agreements	EKM-02.1 EKM-03.1 GRM- 06.1 GRM- 06.1 GRM- 09.1 GRM- 09.1 HRS-01.1 HRS-02.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business rold/nuclicon and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you polity our lenants when your make material changes to your information security and/or privacy policies? Upon termination of contract or business relationship, are employees and business patheres adequately informed of their obligations for returning organizationally-cowned assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? Do your enflyoment agreements incorporate provisions and/or terms in adherence to established information governance and security policies? Are documented policies, procedures, and guidelines in place to gover change in employment and/or termination?	Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts
Governance and Risk Management	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination Training / Awareness	EKM-02.1 EKM-03.1 GRM- 06.1 GRM- 06.1 GRM- 09.2 HRS-01.1 HRS-03.1 HRS-03.1 HRS-04.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g. hypervisors, operating systems, routers, DNS servers, etc.]? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business rolefunction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security nolicies and procedures? Do you portal your tenants when you make material changes to your information security and/or privacy policies? Do you portavy mathing and reviews to your privacy and security policies? Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizational/yourent candidates, contractors, and involved third parties subject to background verification? Do you enform, exerting provers policies? Andernece to established information governance and security policies? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment and/dates, contractors, and involved third parties subject to background verification? Do you enform and the obligations for returning organizationally tablished information governance and security policies? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Do your estrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, management systems (e.g., hypervisors, firewalls, vulnerability scanners, fi	Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination	EKM-02.1 EKM-03.1 GRM- 06.1 GRM- 06.1 GRM- 09.2 HRS-01.1 HRS-03.1 HRS-03.1 HRS-04.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business roldruction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you perform, at minimum, annual reviews to your privacy and security unformation security and/or privacy policies? Upon termination of contract or business relationship, are employees and business pathers adequately informed of their obligations for returning organizationally-owned assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment andidates, contractors, and involved tind parties subject to background verification? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Are personnet trained and provided with awareness programs at least once a year? Do your ensify and/or termination?	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination Training / Awareness	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 05.1 GRM- 09.2 HRS-01.1 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 IAM-01.2	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you nave documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business rolefunction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security outcles and procedures? Do you entry unitenants when your make material changes to your information security and/or privacy policies? Do you porting unitenants when your make material changes to your policies? Upon termination of contract or business relationship, are employees and business patheres adequately informed of their obligations for returning organizationally-covined assets? Pursuant to local ways, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? Are posument doynemating over angle end security policies? Are documented policies, procedures, and guidelines in place to gover change in employment adject memation? Are positioned trained and provided with awareness programs at least once a year? Do you estrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalts, vulnerability scanners, networks antifes, Ale, sec.)?	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Agreements Training / Awareness Audit Tools Access	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 05.1 GRM- 09.2 HRS-01.1 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 IAM-01.2	Do yu estrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environmen? Do you encrypt tenant data at rest (on disk/storage) within your environmen? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.]? Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business rolefunction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security colicies and procedures? Do you porting a timinium, annua relevise to your privacy and security policies? Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-word assets? Parsuant to local laws, reglations, etitics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? Do you erform and/or termination? Are document policies, provident, and guidelines in place to goven change in employment and/or termination? Do you montry field, and monitor access to your information security Do you monter (e.g., hypervisors, firewalls, widensbuilty sciences a yuar? Do you monter (e.g., hypervisors, firewalls, widensbuilty sciennes, network sinffers, APIs, etc.)? Do you monter and log privileged access (e.g. administrator (evel) to information security management systems? Do you wange and store the identity of all personnel who have access that is no longer required for business purposes? Do you wange and store the identity of all personnel who have	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Security and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Agreements Employment Agreements Training / Awareness Audit Tools Access User Access Policy Policies and Procedures	EKM-02.1 EKM-03.1 GRM- 05.1 GRM- 09.1 GRM- 09.1 GRM- 09.2 HRS-01.1 HRS-01.1 HRS-02.1 HRS-03.1 HRS-04.1 HRS-04.1 IAM-01.2 IAM-01.1	Do yu certicic physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environmen? Do you information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/nuction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you notify your tenants when you make material changes to your information security and/or privacy policies? Do you polity you tenants when you make material changes to your information security and/or privacy policies? Do you polity owned haves relationship, are employees and business partners adequately informed of their obligations for returning organizationality-owned assets? Pursuant to local waw, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? Do you retrict, log, and monitor access to your information security policies? Do you restrict, log, and monitor access to your information security management systems (e.g., hypenisors, firewalls, vulnerability scenners, network sniffers, APIs, etc.)? Do you restrict, log, and monitor access (e.g., administrator level to information security management systems? Do you manage and store the identity of all personnel who have access to the firstructure, including their level of access? Are controls in place to prevent unautonized access to your application, program, or object source code, and assure it is restricted to authorized	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Security and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination Training / Awareness Audit Tools Access User Access Policy	EKM-02.1 EKM-03.1.3 GRM- 05.1 GRM- 05.1 GRM- 09.2 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-03.1 IAM-01.2 IAM-01.2 IAM-02.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security basclines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, et.)? A rey our information security policies and procedures made available to all impacted personnel and business partners, authorized by a accountable business rold/nuclicon and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you polity our lenants when your make material changes to your information security prince privacy policies? Do you polity our lenants when your make material changes to your information security and/or privacy policies? Upon termination of contract or business relationship, are employees and business pathres adequately informed of their obligations for returning organizationally-cowind assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? Are personnet tailed and provided with avareness programs at least once a year? Do you unotify and/or termination? Are appressing to local og privilege access (e.g., administrator level) to information security management systems? Do you monitor allog privilege access (e.g., administrator level) to information security management systems? Do you mange and store the identity of all personnel who have access to the fi information security management systems? Do you mange to tore to set u	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Stipulated in employment contracts Scurity and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access package requests that are reviewed. Offboarding policies ensure access is removed.
Governance and Risk Management Human Resources	Key Generation Encryption Encryption Baseline Requirements Policy Policy Enforcement Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Agreements Employment Training / Awareness Judit Tools Access User Access Policy Policies and Procedures Source Code Access	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 05.1 GRM- 09.2 HRS-01.1 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-04.1 HRS-04.1 IAM-01.1 IAM-01.2 IAM-02.1 IAM-02.1	Do you restrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environmen? Do you encrypt tenant data at rest (on disk/storage) within your environmen? Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/nuction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? Do you notify you tenants when you make material changes to your information security and/or privacy policies? Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning arganizationally-owned assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? Do you retrict, log, and monitor access to puri information security partices? Do you information do provide with awareness programs at least once a year? Do you restrict, log, and monitor access to your information security management systems? Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalts, vulnerability scanners, network sinffers, APIs, etc.)? Do your monitor and to privileged access (e.g., administrator level) to information security in place ensuming timely removal of systems access that is no longer required for business purposes? Do you monitor and to privileged access? Are controls in	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Stipulated in employment contracts Scurity and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access package requests that are reviewed. Offboarding policies ensure access is removed.
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination Training / Awareness Audit Tools Access User Access Policy Policies and Procedures Source Code Access Restriction /	EKM-02.1 EKM-03.1 GRM- 01.1 GRM- 05.1 GRM- 09.2 HRS-01.1 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-04.1 HRS-04.1 IAM-01.1 IAM-01.2 IAM-02.1 IAM-02.1	Do yu certicic physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of you infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/nuccion and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security oulcies and procedures? Do you enotity out enants when your make material changes to your information security and/or privacy policies? Upon termination of contract or business relationship, are employees and business pathematical axes, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third paties subject to backgrount writefation? Do you entify moment and/or termination? Are personnel trained and provided with awareness programs at least once a year? Do you restrypment adjectemation? Are personnel trained and provided with awareness programs at least once a year? Do you write youngent adject termination? Are personnel trained and provided with awareness programs at least once a year? Do you write mailers, hypervisors, firewalls, winerability scanners, network sinters, Ale, stc.? D Do you monitor and log privileged access (e.g., administrator level to information secure you.g., hypervisors, firewalls, winerability scanners, networks sinters, Ale, stc.? D Do you monitor and log private youngent, and we access to the information secure code, and assure it is restricted to authorized personnet	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Stipulated in employment contracts Scurity and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access package requests that are reviewed. Offboarding policies ensure access is removed.
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination Training / Awareness Audit Tools Access User Access Policy Policies and Procedures Source Code Access Restriction /	EKM-02.1 EKM-03.1.1 GRM- 05.1 GRM- 09.1 GRM- 09.2 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-03.1 IAM-01.1 IAM-01.2 IAM-01.1 IAM-04.1 IAM-06.1	Do yu estrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environmen? Do you information accurity baselines for every component of your information security baselines for every component of your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business rolefunction and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security and/or privacy policies? Do you portify jour tenants when you make material changes to your information security and/or privacy policies? Do you portify nour tenants when you make material changes to your information security and/or privacy policies? Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-womed assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment and/or termination? Do you enforting and monitor access to your information security policies? Uno termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-womed assets? Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment and/or termination? Do you enstrict, log, and monitor access to your information security Do you estrict, log, and monitor access to your information security Do you monitor access (e.g. a, diministrator level) to information security management systems? Do you manage and store the identity of all personnel who have access to the f1 infrastructure, including their level of access? Are controls in place to	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Stipulated in employment contracts Scurity and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access package requests that are reviewed. Offboarding policies ensure access is removed.
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination Training / Awareness Audit Tools Access User Access Policy Policies and Procedures Source Code Access Restriction / Authorization	EKM-02.1 EKM-03.1.1 GRM- 05.1 GRM- 09.1 GRM- 09.2 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-03.1 IAM-01.1 IAM-01.2 IAM-01.1 IAM-04.1 IAM-06.1	Do yu certicic physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you navy documented information security baselines for every component of you infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/nuclicon and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security oulcies and procedures? Do you ontity out enants when your make material changes to your information security and/or privacy policies? Upon termination of contract or business relationship, are employees and business pathematical ands, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third paties subject to background verification? Do you entify ungent advice thermitation of contract or business nature to established information governate and security policies? Are documented policies, procedures, and guidelines in place to govern change in employment advice termination? Are personnel trained and provided with awareness programs at least once a year? Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalis, vuinerability scanners, networks siffes, Ale, stc.)? Do you nomitor and log privileged access (e.g., administrator level to information ecurity management systems? Do you manage and store the identity of all personnel who have access to the information secure source code, and assure it is restricted to a uthorized personnel only? Do you require a periodical authorized access to tenant application, prog	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Customer-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Stipulated in employment contracts Scurity and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access package requests that are reviewed. Offboarding policies ensure access is removed.
Governance and Risk Management Human Resources	Key Generation Encryption Baseline Requirements Policy Policy Enforcement Policy Enforcement Policy Reviews Asset Returns Background Screening Employment Termination Training / Awareness Audit Tools Access User Access Policy Policies and Procedures Source Code Access Restriction / Authorization	EKM-02.1 EKM-03.1.1 GRM- 05.1 GRM- 09.1 GRM- 09.2 HRS-01.1 HRS-03.1 HRS-03.1 HRS-03.1 HRS-03.1 IAM-01.1 IAM-01.2 IAM-01.1 IAM-04.1 IAM-06.1	Do yu estrict physical access to information assets and functions by users and support personnel? Do you have a capability to allow creation of unique encryption keys per tenant? Do you encrypt tenant data at rest (on disk/storage) within your environment? Do you have documented information security baselines for every component of you infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? A key our information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/nuclicon and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)? Is a formal disciplinary or sanction policy established for employees who have violated security oulcies and procedures? Do you notify your tenants when your make material changes to your information security and/or privacy policies? Do you policy untenants when your make material changes to your information security and/or privacy policies? Do you policy untenants when your privacy and security policies? Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets? Pursuant to local taws, regulations, ethics, and contractual constraints, are all employment and/ot termination? Are personnel trained and provided with awareness programs at least once a year? Do you restrict, log, and monitor access to your information security management systems (e.g., hypenvisor, firewalls, vulnerability scenners, management systems (e.g., hypenvisor, firewalls, vulnerability scenners, metwork snifters, APIs, etc.)? Do you monitor and log privileged access to your application, program, or object source code, and assure it is restricted to authorized personnel only? Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel onl	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Custome-provided files and customs proposal output is encrypted at rest in separate containers and keys for each tenants, these are platform managed. Provided and enabled by our cloud providers We are ISO 27001 certified. Stipulated in employment contracts Stipulated in employment contracts Stipulated in employment contracts Security and ISO 27001 awareness training and campaigns occur at least once a year. For engineers, additional secure software training is required. Quarterly access review workflows, roles are requested through temporary access package requests that are reviewed. Offboarding policies ensure access is removed.

Audit Logging / Intrusion Audit Logging / Intrusion Are file integrity (host) and network intrusion detection (IDS) tools Yes Presented to help facilitate timely detection, investigation by root cause analysis, and response to incidents? Yes IT personnel IVS-01.1 Is physical and logical user access to audit logs restricted to authorized (IVS-01.5) Yes IT personnel Visco 11 Is physical and logical user access to audit logs restricted to authorized (IVS-01.5) Yes IT personnel Option 201 Preson 201 Preson 201 Preson 201 Preson 201 Option 201 Preson 201 Preson 201 Preson 201 Preson 201 Option 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201 Preson 201	
Audit Logging / Intrusion Detection analysis, and response to incidents? Image: Comparison of the system of the s	
Detection Its Spisal and logical user access to audit logs restricted to authorized Yes IT personnel IvS 01.2 Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)? Yes At least once every quarter	
IVS-01.5 Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)? Yes At least once every quarter Do avourse a supprovided time senders protocol (e.g., NTD) to ansure all. Yes At least once every quarter	
(1930) a automated tools/?	
Cleak Superscription Do you use a synchronized time-service protocol (e.g., NTP) to ensure all Yes AD clock synchronization	
systems have a common time reference? Are operating systems hardened to provide only the necessary ports, Yes	
OS Hardening and Base use protocols, and services to meet business needs using technical controls (e.g.,	
Controls antivirus, file integrity monitoring, and logging) as part of their baseline build	
standard or template? Production / Non. Vis. no.1 For your SaaS of PaaS offering, do you provide tenants with separate Yes	
Production Production and test processes?	
Environments IVS-08.3 Do you logically and physically segregate production and non-production Yes environments	
environments protected by a firewall or virtual Yes	
Segmentation IVS-09.1 firewall to ensure business and customer security requirements?	
Do you restrict personnel access to all hypervisor management functions or Yes	
administrative consoles for systems hosting virtualized systems based on the	
VMM security - IVS-11.1 principle of least privilege and supported through technical controls (e.g., two-	
Hypervisor Hardening factor authentication, audit trails, IP address filtering, firewalls and TLS-	
encapsulated communications to the administrative consoles)?	
Are policies and procedures established and mechanisms configured and Yes	
implemented to portect the wireless network environment perimeter and to	
restrict unauthorized wireless traffic?	
Are policies and procedures established and mechanisms implemented to Yes	
ensure wireless security settings are enabled with strong encryption for Wireless Security IVS-12.2 authentication and transmission, replacing vendor default settings (e.g.,	
erception keys, passwords, SMPC community strings?	
Are policies and procedures established and mechanisms implemented to Yes	
IVS-12.2, protect writests indevice involvements and catect unpresence of unauthorized (rogue) network devices for a timely disconnet from the	
network?	
teroperability & Portability apps lipy-01.1 Do you publish a list of all APIs available in the service and indicate which are to service and indicate which are ustomized?	pecification - all APIs are considered standard
	is limited to ops communication (notification
Approved Applications MOS-03.1 approved applications and those from approved application stores can be or text to notify of incidents)	
Icaded onto a mobile device? ecurity Incident Management, E- SEF-02.1 [Do you have a documented security incident response plan? Yes	
iscovery, & Cloud Forensics Indent Management SEF-0.2.4 Have you tested your security incident response plans in the last year? Yes	
Are workforce personnel and external business relationships adequately Yes	
SEF-03.1 Informed of their responsibility, and, if required, consent and/or contractually	
required to report all information security events in a timely manner?	
Incident Reporting	icated and tested during onboarding process
Incident Reporting Do you have predefined communication channels for workforce personnel Yes Support helpdesk procedures are commun	icated and tested during onboarding process
Incident Reporting Do you have predefined communication channels for workforce personnel Yes Support helpdesk procedures are commun	icated and tested during onboarding process
Incident Reporting Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel adhering to applicable legal, statutory, or regulatory compliance obligations?	icated and tested during onboarding process
Incident Reporting Do you have predefined communication channels for worldorce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication shared Incident Response Legal Preparation SEF-04.4 Do you enforce and attest to tenant data separation when producing data in eresponse to legal subpoenas? Yes In case of legal subpeona we will ensure th shared	
Incident Reporting preparation Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes In case of legal subpeona we will ensure the shared upply Chain Management, Transparency, An external Do you make security incident information available to all affected customers Yes Our customers will be informed via mail.	
Incident Reporting preparation Op you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes In case of legal subpeona we will ensure the shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you make security incident information available to all affected customers Yes Our customers will be informed via mail.	
Incident Reporting Do you have predefined communication channels for worldorce personnel and entry the predefined communication channels for worldorce personnel and entry manner and entry to policable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for worldorce personnel and entry manner and entry to policable legal, statutory, or regulatory compliance obligations? Yes In case of legal subpeona we will ensure th shared upply Chain Management, Transparency, nd Accountability Incident Reporting STR-02.1 Do you collect capacity and used ata for all relevant components of your Yes Ves upply Chain Management, Transparency, nd Accountability Incident Reporting STR-02.1 Do you collect capacity and use data for all relevant components of your Yes	
Incident Reporting Incident Reporting Preparation Image: Do you have predefined communication channels for workforce personnel and estimate business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication and estimate business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes In case of legal subpeona we will ensure the shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)? Yes Our customers will be informed via mail.	
Incident Reporting preparation Incident Reporting EFF-02 Do you have predefined communication channels for workforce personnel and extrnal business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication ashered upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you make security incident information available to all affected customes Yes In case of legal subpeona well ensure the shared Network / Infrastructure Services STA-02.1 Do you make security incident information available to all affected customes Yes Our customers will be informed via mail. Network / Infrastructure Grudo STA-02.1 Do you make security indicent information available to all affected customes Yes All third parties we work with are ISO2700 Network / Infrastructure Grudo STA-02.4 Do third-party agreements include provision for the security and protection of Yes All third parties we work with are ISO2700	at solely data required for the subpoena will be
Incident Reporting Op you have predefined communication channels for workforce personnal and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner response to legal subponas and external business partners to report incident information available to all affected customers in a timely manner and external business partners to report incident information available to all affected customers in a timely manner and providers periodically through electronic methods (e.g., portals)? Yes Our customers will be informed via mail. Network / Infrastructure services ST-02.1 Do you collect capacity and ue data for all relevant components of your services of energy excercises and providers periodically through electronic methods (e.g., portals)? Yes Our customers will be informed via mail. Network / Infrastructure services ST-02.1 Do you collect capacity and ue data for all relevant components of your Yes Ves In customers will be informed via mail. Nitrid Party Agreements ST-02.1 Do you collect capacity and ue data for all relevant components of your Yes All third parties we work with are IS02700 information and assets? <td>at solely data required for the subpoena will be</td>	at solely data required for the subpoena will be
Incident Reporting Do you have predefined communication channels for workforce personnel Yes Support helpdesk procedures are communication channels for workforce personnel upply Chain Management, Transparency, nd Accountability Incident Reporting SEF-04.2 Do you enforce and attest to tenant data separation when producing data in response to legal subpeonse to leg	at solely data required for the subpoena will be
Incident Reporting Incident Reporting Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel and external business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel and external business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication when producing data in providence obligations? upply Chain Management, Transparency, nd Accountability Incident Reporting SFR-03.2 Do you make security incident information available to all affected customers Yes Our customers will be informed via mail. Network / Infrastructure Services STA-03.1 Do you collect capacity and use data for all relevant components of your Yes Our customers will be informed via mail. Third Party Agreement STA-03.1 Do you collect capacity and use data for all relevant components of your Yes All third parties we work with are ISO2700 information and assets? Third Party Agreement STA-03.1 Do typu row the capability to recover data for a specific customer in the case	at solely data required for the subpoena will be
Incident Reporting Incident Reporting Do you have predefined communication channels for workforce personnal and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incident information available to all affected customers in shared Yes In case of legal subpeona well ensure the shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you make security incident information available to all affected customers is shared Yes Our customers will be informed via mail. Network / Infrastructure service STA-02.1 Do you collect capacity and use data for all relevant components of your Yes Our customers will be informed via mail. Network / Infrastructure service and relevant components of your Yes All third parties we work with are ISO2700 in and assets? Third Party Agreements STA-05.1 Do third-party agreements include provision for the security and protection of a failure or data loss? Yes All third part	at solely data required for the subpoena will be
Incident Reporting Incident Reporting Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel and external business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel and external business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication when producing data in providence obligations? upply Chain Management, Transparency, nd Accountability Incident Reporting SFR-03.2 Do you make security incident information available to all affected customers Yes Our customers will be informed via mail. Network / Infrastructure Services STA-03.1 Do you collect capacity and use data for all relevant components of your Yes Our customers will be informed via mail. Third Party Agreement STA-03.1 Do you collect capacity and use data for all relevant components of your Yes All third parties we work with are ISO2700 information and assets? Third Party Agreement STA-03.1 Do typu row the capability to recover data for a specific customer in the case	at solely data required for the subpoena will be
Incident Reporting Do you have predefined communication channels for workforce personnal and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incident separation when producing data in preparation when producing data in the shared Yes Support helpdesk procedures are communication when producing data in shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you make security incident information available to all affected customers shared Yes Our customers will be informed via mail. Network / Infrastructure Services STA-02.1 Do you collect capacity and use data for all relevant components of your Yes All third parties we work with are ISO2700 information and assets? Third Party Agreements STA-03.1 Do you provide teanst shreed in droigned visibility and reporting of your Yes All third parties we work with are ISO2700 information and assets? Third Party Agreements STA-03.1 Do third-party agreements include provision for the security and protection of information and assets? Yes All third parties we work with are ISO2700 information and assets?	at solely data required for the subpoena will be
Incident Reporting Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable (egal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you enforce and attest to team t data separation when producing data in regoness to legal subpoenas? Yes In case of legal subpeona we will ensure th shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you collect capacity incident information available to all affected customers services Yes Our customers will be informed via mail. Network / Infrastructure Services STA-02.1 Do you collect capacity and use data for all relevant components of your services Yes All third parties we work with are ISO2700 information and assets? Third Party Agreements STA-03.1 Do you provide tenants with and segarity or to recover data for a specific customer in the case Yes All third parties we work with are ISO2700 information and sests? Third Party Audits STA-07.4 Do train dassets? Do you provide tenants with organity subbility and reporting dryour Yes Available on demand Do you have the capability to party provide tenant statuseqdry on security r	at solely data required for the subpoena will be
Incident Reporting Opyout have predefined communication channels for workforce personnel and acternal business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication channels for workforce personnel and acternal business partners to report incidents in a timely manner andering to applicable legal, statutory, or regulatory compliance obligations? Yes Incase of legal subpeona ve will ensure the shared upply Chain Management, Transparency, nd Accountability Incident Reporting SF-04.2 Do you onloce and attest to team t data separation when producing data in shared Yes Our customers will be informed via mail. Network / Infrastructure Services STA-02.1 Do you collect capacity and use data for all relevant components of your Yes Our customers will be informed via mail. Intrid Party Agreements STA-03.1 Do you collect capacity and use data for all relevant components of your Yes All third parties we work with are ISO2700 in a failure or data loss? Third Party Agreements STA-03.2 Do you provide tenants with ongoing visibility and reporting of your Yes All third parties we work with are ISO2700 in a failure or data loss? Third Party Audits STA-07.4 Do you provide tenants with ongoing visibility and reporting of your Yes Available on demand	at solely data required for the subpoena will be
Incident Reporting Incident Reporting Do you have predefined communication channels for workforce personnal and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents in a timely manner and external business partners to report incidents (e.g., statutory, or regulatory compliance obligations?) Yes Import heighdesk procedures are communication when producing data in shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02.1 Do you make security incident information available to all affected customers set information and a providers periodically through electronic methods (e.g., portals)? Ves Our customers will be informed via mail. Network / Infrastructure Services STA-02.1 Do you collect capacity and use data for all relevant components of your Yes All third parties we work with are ISO2700 indication and assets? Thrid Party Agreements STA-05.1 Do third-party agreements include provision for the security and protection of a failure or data loss? Yes All third parties we work with are ISO2700 indications? Thrid Party Agreements STA-05.1 Do tyou provide tenants with orgonity visibility and reportin	at solely data required for the subpoena will be
Incident Reporting Incident Reporting Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02. Do you enforce and attest to team t data separation when producing data in regoness to legal subpoenas? Yes In case of legal subpeona we will ensure th shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02. Do you collect capacity incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)? Ves Our customers will be informed via mail. Network / Infrastructure services STA-02. Do you collect capacity and use data for all relevant components of your services Yes All third partles we work with are ISO2700 information and assets? Third Party Agreements STA-03.1 Do you provide teams through on going visibility and reporting of your af a latific or data loss? Yes All third partles we work with are ISO2700 information and assets? Third Party Agreements STA-03.1 Do bur collect capacity and use data for a specific customer in the case of a failure or data loss? Yes Ault hird partles we work with ar	at solely data required for the subpoena will be
Incident Reporting Incident Reporting Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? Yes Support helpdesk procedures are communication shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02. Do you enforce and attest to team t data separation when producing data in regoness to legal subpoenas? Yes In case of legal subpeona we will ensure th shared upply Chain Management, Transparency, nd Accountability Incident Reporting STA-02. Do you collect capacity incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)? Ves Our customers will be informed via mail. Network / Infrastructure services STA-02. Do you collect capacity and use data for all relevant components of your services Yes All third partles we work with are ISO2700 information and assets? Third Party Agreements STA-03.1 Do you provide teams through on going visibility and reporting of your af a latific or data loss? Yes All third partles we work with are ISO2700 information and assets? Third Party Agreements STA-03.1 Do bur collect capacity and use data for a specific customer in the case of a failure or data loss? Yes Ault hird partles we work with ar	at solely data required for the subpoena will be